CLAIMS

1. A prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising:

a prime storage unit storing the known prime q;

a management information storage unit storing unique management information;

a random information generation unit operable to read the management information from the management information storage unit, and generate random information R based on the read management information;

a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N according to $N = 2 \times$ random information $R \times$ prime $q + 1$;

a primality testing unit operable to test primality of the calculated prime candidate N; and

an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined.

2. The prime calculating apparatus of Claim 1, wherein

the random information generation unit includes:

a reading subunit operable to read the management information from the management information storage unit;

a random number calculation subunit operable to calculate a random number r;

a combining subunit operable to make a combination of the read management information and the generated random number r;

and

a computation subunit operable to compute the random information R based on the combination.

3. The prime calculating apparatus of Claim 2, wherein

the computation subunit computes the random information R by applying an injection function to the combination.

4. The prime calculating apparatus of Claim 3, wherein

the injection function is an exclusive OR, and

the computation subunit prestores predetermined key information, and computes the random information R by applying the exclusive OR to the key information and the combination.

5. The prime calculating apparatus of Claim 3, calculating the prime candidate N having a bit length twice a bit length of the prime q, wherein

the random number calculation subunit calculates the random number r, a bit size of which is obtained by subtracting a bit length of the management information and 1 from the bit length of the prime q.

6. The prime calculating apparatus of Claim 5, wherein

the primality testing unit includes:

a 1st judging subunit operable to judge whether the prime candidate N satisfies $2^{N-1} = 1 \ mod \ N$; and

a 2nd judging subunit operable to perform, when the judgment of the 1st judging subunit is affirmative, a judgment of whether the prime candidate N and the random information R satisfy 2^{2R}

$\neq 1 \ mod \ N$, and to determine the primality of the prime candidate N when the performed judgment is affirmative.

7. The prime calculating apparatus of Claim 5, wherein

the primality testing unit includes:

a 1st judging subunit operable to judge whether prime candidate N satisfies $2^{N-1} = 1 \ mod \ N$; and

a 2nd judging subunit operable to perform, when the judgment of the 1st judging subunit is affirmative, a judgment of whether prime candidate N and random information R satisfy $GCD(2^{2R}-1, N) = 1$, and to determine the primality of prime candidate N when the performed judgment is affirmative.

8. The prime calculating apparatus of Claim 1, further comprising:

an iteration control unit operable to control the random information generation unit, the candidate calculation unit, and the primality testing unit to iterate the generation of the random information R, the calculation of the prime candidate N, and the primality testing until the primality of the calculated prime candidate N is determined by the primality testing unit.

9. The prime calculating apparatus of Claim 8, further comprising:

a secondary random number calculation unit operable to calculate a random number R';

a secondary candidate calculation unit operable to calculate a prime candidate N', according to $N' = 2 \times$ random number $R' \times$ prime $N + 1$, using the output prime N and the calculated random number R';

a secondary primality testing unit operable to test primality

of the calculated prime candidate N';

a secondary output unit operable to output the calculated prime candidate N' as a prime when the primality of the calculated prime candidate N' is determined; and

a secondary iteration control unit operable to control the secondary random number calculation unit, the secondary candidate calculation unit, and the secondary primality testing unit to iterate the calculation of the random number R', the calculation of the prime candidate N', and the primality testing until the primality of the calculated prime candidate N' is determined by the secondary primality testing unit.

10. The prime calculating apparatus of Claim 8, further comprising:

a secondary information storage unit storing a predetermined verification value;

a secondary random number generation unit operable to generate a random number r'; and

a secondary candidate calculation unit operable to calculate random information R' by multiplying the management information by the generated random number r', and calculate a prime candidate N' according to $N' = 2 \times$ random information $R' \times$ prime $N +$ the verification value, wherein

the primality testing unit further tests primality of the calculated prime candidate N', and

the output unit further outputs the calculated prime candidate N' as a prime when the primality of the calculated prime candidate N' is determined.

11. The prime calculating apparatus of Claim 8 that is a key generating apparatus for generating a public key and a private key of RSA encryption, further comprising:

a public key generation unit operable to generate the public key using the prime N; and

a private key generation unit operable to generate the private key using the generated public key.

12. The prime calculating apparatus of Claim 11, wherein

the public key generation unit (i) directs the iteration control unit to newly obtain a prime N', (ii) calculates a number n, according to n = prime $N \times$ prime N', using the prime N and the newly obtained prime N', and (iii) generates a random number e,

a combination of the calculated number n and the generated random number e is the public key,

the private key generation unit calculates d satisfying $e \times d = 1 \ mod \ L$,

L is a least common multiple of the prime N - 1 and the prime N' - 1, and

the calculated d is the private key.

13. The prime calculating apparatus of Claim 11 that is a key issuing server apparatus for generating and issuing the private key and the public key of RSA encryption for a terminal, further comprising:

a key output unit operable to output the generated private key to the terminal; and

a publishing unit operable to publish the generated public key.

14. The prime calculating apparatus of Claim 13, further comprising:

an identifier obtaining unit operable to obtain a terminal identifier uniquely identifying the terminal;

a management information generation unit operable to generate the management information including the obtained terminal identifier; and

a writing unit operable to write the generated management information to the management information storage unit.

15. The prime calculating apparatus of Claim 14, further comprising:

a server identifier storage unit prestoring a server identifier uniquely identifying the prime calculating apparatus functioning as the key issuing server apparatus, wherein

the management information generation unit further reads the server identifier from the server identifier storage unit, and generates the management information further including the read server identifier.

16. A prime calculating apparatus for calculating a prime larger than a known prime, comprising:

a prime calculation unit operable to calculate an output prime having a bit length twice a bit length of a known input prime;

a prime storage unit storing an initial value of the known prime; and

an iteration control unit operable to control the prime calculation unit to perform the calculation a plurality of iteration rounds, wherein

the iteration control unit gives, in a first iteration round, the initial value to the prime calculation unit as the input prime, while

giving, in each of the rest of the plurality of iteration rounds, an output prime calculated in an immediately preceding round to the prime calculation unit as the input prime, and

in one of the plurality of iteration rounds, the prime calculation unit includes:

a management information storage subunit storing unique management information;

a random information generation subunit operable to read the management information from the management information storage subunit, and generate a random information R based on the read management information;

a candidate calculation subunit operable to receive the input prime, and calculate a prime candidate N according to N = 2 × random information R × the input prime + 1;

a primality testing subunit operable to test primality of the calculated prime candidate N;

an output unit operable to output the calculated prime candidate N as the output prime when the primality of the calculated prime candidate N is determined; and

an iteration control subunit operable to control the random information generation subunit, the candidate calculation subunit, and the primality testing subunit to iterate the generation of the random information R, the calculation of the prime candidate N, and the primality testing until the primality of the calculated prime candidate N is determined by the primality testing subunit.

17. The prime calculating apparatus of Claim 16, wherein

in a last iteration round, the prime calculation unit includes:

an information storage subunit storing a predetermined verification value;

a random number generation subunit operable to generate a random number r';

a candidate calculation subunit operable to calculate random information R' by multiplying the management information by the generated random number r', and calculate a prime candidate N' according to $N' = 2 \times$ random information $R' \times$ the output prime calculated in an immediately preceding round + the verification value;

a primality testing subunit operable to test primality of the calculated prime candidate N';

an output subunit operable to output the calculated prime candidate N' as the output prime when the primality of the calculated prime candidate N' is determined; and

an iteration control subunit operable to control the random number generation unit, the candidate calculation unit, and the primality testing unit to iterate the generation of the random number r', the calculation of the prime candidate N', and the primality testing until the primality of the calculated prime candidate N' is determined by the primality testing subunit.

18. A key issuing system including a terminal and a key issuing server apparatus for generating and issuing a private key and a public key of RSA encryption for the terminal, wherein

the key issuing server apparatus comprises:

a prime calculation unit operable to calculate a prime N larger than a known prime q;

a public key generation unit operable to generate the public

key using the calculated prime N;

a private key generation unit operable to generate the private key using the generated public key;

a key output unit operable to output the generated private key to the terminal; and

a publishing unit operable to publish the generated public key,

the prime calculation unit includes:

a prime storage subunit storing the known prime q;

a management information storage subunit storing unique management information;

a random information generation subunit operable to read the management information from the management information storage subunit, and generate random information R based on the read management information;

a candidate calculation subunit operable to read the prime q from the prime storage subunit, and calculate a prime candidate N according to $N = 2 \times$ random information $R \times$ prime $q + 1$;

a primality testing subunit operable to test primality of the calculated prime candidate N;

an output subunit operable to output the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined; and

an iteration control subunit operable to control the random information generation subunit, the candidate calculation subunit, and the primality testing subunit to iterate the generation of the random information R, the calculation of the prime candidate N, and the primality testing until the primality

of the calculated prime candidate N is determined by the primality testing subunit, and

the terminal includes:

a reception unit operable to receive the private key; and

a key storage unit operable to store the received private key.

19. The key issuing system of Claim 18, further comprising a certificate issuing server apparatus, wherein

the key output unit outputs the public key to the certificate issuing server apparatus, and

the certificate issuing server apparatus includes:

a storage unit storing a private key of the certificate issuing server apparatus;

an obtaining unit operable to obtain the public key;

a certificate generation unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and

an output unit operable to output the generated public key certificate to the key issuing server apparatus.

20. A prime calculation method used in a prime calculating apparatus that calculates a prime candidate N larger than a known prime q and tests primality of the calculated prime candidate N, the prime calculating apparatus including: a prime storage unit storing the known

prime q; and a management information storage unit storing unique management information, the prime calculation method comprising:

a random number generation step of reading the management information from the management information storage unit and generating random information R based on the read management information;

a candidate calculation step of reading the prime q from the prime storage unit, and calculating the prime candidate N according to N = 2 × random information R × prime q + 1;

a primality testing step of testing primality of the calculated prime candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined.

21. A prime-calculation computer program used on a prime calculating apparatus that calculates a prime candidate N larger than a known prime q and tests primality of the calculated prime candidate N, the prime calculating apparatus including: a prime storage unit storing the known prime q; and a management information storage unit storing unique management information, the prime-calculation computer program comprising:

a random number generation step of reading the management information from the management information storage unit and generating random information R based on the read management information;

a candidate calculation step of reading the prime q from the prime storage unit, and calculating the prime candidate N according to N = 2 × random information R × prime q + 1;

a primality testing step of testing primality of the calculated

prime candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined.

22. The prime-calculation computer program of Claim 21 stored in a computer-readable recording medium.

23. The prime-calculation computer program of Claim 21 to be transmitted on a carrier wave.